Annual ADFSL Conference on Digital Forensics, Security and Law

2009
Proceedings

May 22nd, 9:00 AM

Cybercrime and the 2012 London Olympics

Denis Edgar-Nevill
Canterbury Christ Church University, North Holmes Rd, Canterbury CT1 1QU United Kingdom, denis.edgar-nevill@canterbury.ac.uk

Cybercrime and the 2012 London Olympics

Denis Edgar-Nevill
Canterbury Christ Church University
North Holmes Rd, Canterbury CT1 1QU United Kingdom
Tel +44 (0) 1227 782089
Email denis.edgar-nevill@canterbury.ac.uk

ABSTRACT

The London 2012 Olympics is just three years away and the clock is ticking to put in place plans get it right. The potential for cybercrime to cause harm during this event is very great; harm to national reputation, harm to the reputation to the Olympic movement, and harm to individuals competing, watching or officiating. This paper considers the need to address these risks by taking a look at what has happened in the past at sporting events and the rising wave of electronic security threats and fraud facilitated by computers at recent Olympics. The problems for law enforcement are discussed surrounding the need to capture and preserve computer forensics data from such a complex live system. The paper concludes by considering the remaining imponderable factors which remain for groups being established by the UK Government to consider.

Keywords Cybercrime, Forensics, Olympics, London, 2012

1. INTRODUCTION

We now live in a world where every large event, bringing the focus of attention of a worldwide audience of hundreds of millions of people, is a target. Any matters surrounding the preparation, planning, resourcing, logistics, financing, development, building, staffing, organisation and delivery becomes a matter for press and public scrutiny. The Olympic Games is a global phenomenon and at a greater risk than many events. Very high in everyone's consciousness are the consequences of terrorist actions seeking "the oxygen of publicity" (Thatcher 1985) with demonstrations of their ability to cause disruption and harm. The attack on the Twin Towers in New York remains as one of the turning-points in history; summarised for all time by the reference to "9/11".

Sports events have been prone to political demonstrations in the past. In 1913 Miss Emily Wilding Davison, a Suffragist, ran on to the course during the race for the Derby and was knocked down by the King's horse. She died from the effects of the injuries she received in Epsom Cottage Hospital a few days later (Morning Post 2009).

The Olympic Games have not been immune to political demonstrations and attacks leading to loss of life.

2. DISRUPTION AT PREVIOUS OLYMPIC GAMES

Mexico 1968

On October 16, 1968, at the Mexico City Olympics, two African-American sprinters Tommie Smith and John Carlos, (gold and bronze medalists, men's 200 metres), raised black-gloved fists on the podium for the medal ceremony as the US national anthem was played. They were both members of the Olympic Project for Human Rights. The "Black Power" salute led to them both being suspended from the US Olympic team and banned from the Olympic Village. ***It was many years before their athletic achievements were finally honored by the US (Slot 2005).***

Munich 1972

In 1972 at the summer games of the XX Olympiad held in Munich, the terrorist group "Black

September" held hostage members of the Israeli Olympic team. As the direct result of a failed rescue attempt when the terrorists attempted to move the hostages at the end of the siege, eleven Israeli's and one German police officer were killed.

Atlanta 1996

On July 27th 1996 the Games of the XXVI Olympiad in Atlanta, Eric Robert Rudolph, former explosives expert for the United States Army, planted the largest pipe bomb in US history in the Centennial Olympic Park. When it exploded at 01.20 am, two people died and 111 were injured. On August 22, 2005, Rudolph was sentenced to three concurrent terms of life imprisonment without parole for the Georgia incidents; on top of a life-sentence for an earlier bomb attack. Rudolph made a statement when sentenced in which he stated that he was angry at the US Government and hoped the Olympics would be cancelled (Gross 2005).

Beijing 2008

The Summer Games of the XXIX Olympiad took place Beijing, China. This venue was always destined to attract demonstration because of the comparatively closed nature of China up until the last decade and international campaigns against perceived breaches of human rights in that country. The run up to the event was marked by a number of human rights demonstrations focused on the repression of the people of Tibet (Wilson et al. 2009) following the invasion of Tibet by China 50 years ago. Less visible than the protests, but potentially every bit as embarrassing, was the dramatic rise in attempts to attack the IT infrastructure of the Beijing Games.

There have been instances of direct electronic attacks on the websites of Olympic Games for at least 20 years with large numbers of security alerts being recorded. The growth in direct attacks during each day of the Beijing Olympics was staggering. One company reported that during each of the days of the Beijing Games there were, on average, in excess of 12 million security alerts. A better way of visualising this is there were around 140 per second, every minute of every hour of every day the Olympic Games in Beijing were open.

Professor Rongsheng Xu (Network Security Group, Institute of High Energy Physics, Chinese Academy of Sciences, China) led the group providing protection to the Beijing website infrastructure and reported that none of these attacks were successful to any significant degree (Xu 2008).

More important perhaps were the crimes reported relating to ticketing fraud. Despite the Chinese government passing laws to make the resale of tickets for Olympic venues illegal tickets were changing hands on online auctioning sites in their thousands. For example, you could have secured a seat at the Opening Ceremony of the Beijing Olympics for around $26,000 (a little more than 40 times the original face value). That is just the sale of tickets which were once legal. Dozens of fake ticket selling sites existed selling unsuspecting athletics fans fake tickets which they only discovered as fake after having travelled to the events in China. Reports of ticketing fraud exceeded $1.5 billion in Europe alone.

3. OPPORTUNITIES FOR CYBERCIME AT THE LONDON 2012 OLYMPICS

Any large event bringing together millions of people is an opportunity for crime. As well as the potential for people to gain notoriety to further a political cause, cybercrime at a distance, with the potential to reach over a billion possible victims, is fast becoming the preferred method of operations for confidence tricksters and thieves.

In September 2008 the British Government announced the creation of a new Police Central e-Crime Unit based within the Metropolitan Police (PCeU 2009). Part of this new units function is to coordinate computer security measures being put into place for the London 2012 Games. This unit has already begun arranging contracts for commercial organisations to provide electronic infrastructure

and security such as Atos Origin (Atos Origin 2009).

Already we have seen the beginnings of cybercrime relating to the 2012 Olympics. The most widespread type email scam which has been received by hundreds of thousands of people is a variation of the lottery scam (Figure 1). Don't expect to claim your prize anytime soon unless you wish to have your bank details stolen!

Figure 1 - 2012 Olympic Lottery Email Scam

In December 2008 the British Computer Society held the inaugural meeting of a new national specialist group in Cybercrime Forensics (Computer Weekly 2009). The BCS Cybercrime Forensics SG (BCS 2009) will advise the society and the professional community on aspects of crime relating to the 2012 Olympics.

4. CYBERCRIME FORENSICS CHALLENGES FOR LONDON 2012

What will be foremost in law enforcement in the run up to and during the 2012 London Olympics will be the need to ensure information vital to computer forensic investigations is not lost:

- **Forensic Computing Data Acquisition and Storage in Real-Time** – capturing data from a live system involving more than a thousand servers and ten thousand PCs spread over 74 venues. On top of that we must also note the Wifi coverage across venues and the potential interactions with hundreds of different types of mobile devices by sportsmen and women, building contractors, officials and spectators;
- **Acting on Forensic Computing Data Acquired in Real-Time** – analysing, fixing flaws and thwarting attacks which might cause damage and might lead to disruption if left unaddressed which constitute the more visible outward signs of attacks;
- **Data Mining Forensic Computing Data** – after it's all over, going back through information gathered to analyse it and trace criminals back to source for future prosecutions.

Each one of these represents a major challenge for law enforcement.

5. ASSESSING THE RISK

Table 1 gives an assessment of the risk of some of the many hundreds of cybercrime types it might be possible to perpetrate against the 2012 London Olympics. The Games are of such high prestige and importance to host countries that the kernel operations of the event itself is very likely to be unaffected by attempts to disrupt it. Perhaps we should 'never say never' but all of the evidence from recent Olympics suggests that core functions will be well protected.

Of growing concern are the attacks which effect individuals rather than the Games themselves where the risks remain very high. Problems such as how do you ensure a fake ticketing site does not domain squat on a name which looks very like the official ticketing site. Olympic organisers already accept that trying to register very variation of domain name which might be used by criminals is an impossible task.

	RISK ITEM	**LIKELYHOOD OF ATTEMPTS**	**LIKELYHOOD OF SUCCESSFUL ATTEMPTS**
MAJOR DISRUPTION DURING THE GAMES	Loss-of-life due to electronic infrastructure misuse	Low?	Very Low
	Suspension of the Games because of systemic electronic infrastructure failures caused by deliberate actions	Very High	Very Low
	Suspension of individual events because of electronic infrastructure failures caused by deliberate actions	Very High	Low
	Loss of coverage for TV Feeds due to misuse or attacks	Medium	Low
	Illegal entry to venues	High	Medium
	Attacks on the Games websites	Very High	Medium
DISRUPTION IN PREPARATION FOR THE GAMES	Fraudulent ticketing using false websites	Very High	Very High
	Online auction merchandising scams using Olympic name	Very High	Very High
	Email scams using the Olympic name	Very High	Very High
LONGER TERM DAMAGE TO REPUTATION	Identity theft using false websites for further fraud	Very High	Very High
	Paedophiles using Olympic blogs, Facebook and other Web 2.0 resources created	Very High	Very High

Table 1: Risks of Cybercrimes at the 2012 Olympics

6. REMAINING IMPONDERABLES

The Games in London are three years away. With reference to Moore's Law, we can reasonably expect the continuing evolution of technology itself to present us with new challenges. Devices will be faster and larger as well as more mobile with greater functionality and connectivity. Developers are playing a continual game of catch up with criminal finding and exploiting weaknesses and flaws in such systems.

What remains true is that, even with the 200,000 hours systems stress-testing the Olympic IT infrastructure being planned by firms such as Altos Origin, it is inconceivable that everything will be perfect.

AUTHOR BIOGRAPHY

Denis Edgar-Nevill holds the post of Head of Department of Computing at Canterbury Christ Church University in the UK. His research includes more than 160 publications and UK and European Union research projects. He is a Fellow of the British Computer Society and member of the BCS Elite group. In 2002 he developed an MSc in Cybercrime Forensics validated with the UK NPIA (National Policing Improvement agency). He chairs the annual CFET (Cybercrime Forensics Education and Training) international conferences and was elected as the founding Chair of the national British Computer Society Cybercrime Forensics Specialist Group in 2008.

REFERENCES

Atos Origin (2009), 'Atos Origin Company website for 2012 Olympics',

http://www.atosorigin.com/en-us/olympic_games/past_future_games/london_2012/default.htm, 18th February 2009

BCS (2009), 'BCS Cybercrime Forensics SG website',

http://www.bcs.org/server.php?show=conWebDoc.23570, 18th February 2009

Computer Weekly (2009) 'BCS Think Tank to Help Protect the 2012 Olympics',

http://www.computerweekly.com/Home/tags/cybercrime-forensics.htm, 18th February 2009

Gross, D. (2005), 'Eric Rudolph lays out the arguments that fueled his two-year bomb attacks', Associated Press, SignonSanDiego.com by the Union-Tribune; April 14, 2005

Morning Post (2009) 'Derby Day Suffragist Incident – Death of Miss Davison, The Morning Post June 9th

1913',http://freepages.genealogy.rootsweb.ancestry.com/~thelamp/sufferage/THE%20MORNING%20POST%20JUNE%209%201913.htm, 18th February 2009

PCeU (2009), 'Police Central e-Crime Unit', http://www.met.police.uk/pceu/index.htm, 18th February 2009

Slot (2005), 'America finally honours rebels as clenched fist becomes salute'. The Sunday Times, UK

Thatcher (1985), Margaret Thatcher – British Prime Minister 1985 Margaret Thatcher Speech

Wilson, S. and Pathitis, N. (2009), 'Tibet Protests Mar Beijing Olympic Plans', ABC News, http://abcnews.go.com/International/WireStory?id=4510954&page=1, 18th February 2009

Xu, R (2008), 'Digital Forensics Research in China', Proceedings of the 2nd International Conference on Cybercrime Forensics Education and Training, Canterbury UK, 1st& 2nd September 2008, ISBN 1899253-19x